FNS FY11 Highlights

Cybersecurity Performance Management (CPM)

- Formulated the FY10 Annual FISMA Congressional Report
- Developed and distributed FY11 FISMA reporting guidance and metrics for federal civilian agencies
- Distributed FISMA results to Federal Executive Branch Agency CIOs/CISOs
- Completed 7 agency CyberStat Reviews and 17 CIO/CISO Interviews
- Completed enterprise-wide analysis of CIO/CISO Interview and CyberScope data

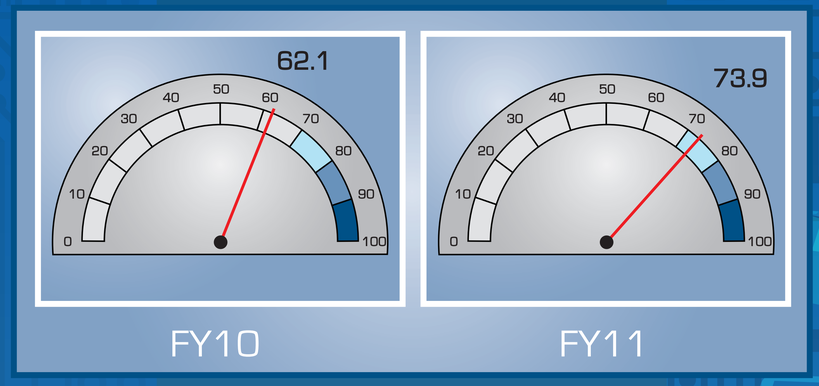
Compliance & Assurance Program (CAP)

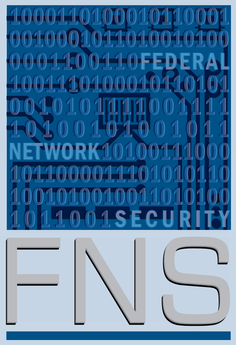
- Completed 18 TICAP agency and 4 MTIPS vendor CCVs
- Initiated RVA and Insider Threat Programs, including a Pilot Assessment with the Federal Aviation Administration (FAA)
- Generated weekly DNSSEC validation scans of the federal enterprise, formalized DNSSEC validation reports, and assisted the DNSSEC Tiger Team
- Defined and executed formal program management process across the organization; resulting in more efficient day-to-day operations

Security Management (SM)

- Planned and executed 2011 Federal Cybersecurity Conference and Workshop and the Continuous Monitoring Track for the 2011 NIST IT Security Automation Conference
- Developed and finalized the Security Management Maturity Questionnaire (SMMQ)
- Managed FNS www.dhs.gov website and created OMB Max Portal instances for the FNS led CISO Advisory Councils
- Conducted RMM pilot assessments with two federal agencies to improve visibility of cyber resiliency

Federal Cybersecurity Posture





FNS

- Increased overall FISMA capabilities from 62.1% in FY10 to 73.9% in FY11
- Established Large and Small Agency CISO Advisory Councils
- Established cybersecurity awards program and recognized top 2 agencies for increased cyber posture
- Drove improvement on 13 out of the 15 FISMA Key Security Metric Capabilities from FY10 to FY11
- Portable device encryption across agencies increased from 54% in FY10 to 83% in FY11
- Government-Wide Continuous Monitoring compliance averages increased from 56.3% in FY10 to 78.3% in FY11
- Improved DNSSEC compliance from 35% in FY10 to 65% in FY11
- Improved email validation technology compliance from 46% to 58%
- Improved 2 factor logical access (HSPD-12) compliance from 55% to 66%
- Improved TIC v1 capabilities compliance from 60% to 72% and TIC traffic consolidation compliance from 48% to 65%

Requirements & Acquisition Support (RAS)

- SAIR Tier 1 BPA netted over $78 Million in cost avoidance in FY11; over $85 Million in total cost avoidance to date
- In collaboration with GSA, awarded 14 BPAs for Risk Management Framework services
- Established HHS and SPAWAR as RMF SSCs
- Co-authored the CAESARS Reference Architecture Framework Extension

Network & Infrastructure Security (N&IS)

- Published the TIC Reference Architecture v2.0 and the TIC 2.0 Implementation Plan
- Engaged with TIC community via two TIC POA&M data calls and two TIC Working Groups
- Published the WLAN, DNS Infrastructure, and CAESARS Reference Architectures
- Launched the Telework/Remote Access, eMail Gateway, and CSATS Reference Architectures
- Supported Government Cloud Computing Efforts (including GSA's FedRamp and the EU-US Cloud Computing Technical Seminar in Brussels)

Project Management Office (PMO)

- Formalized FNS 5-year Strategy, including: the FNS Strategy Map, the FNS Balanced Scorecard, and the FY11 Project Portfolio
- Executed FY11 FNS Budget with a 99.6% obligation rate and prepared FY13-15 FNS Budget Justification. Aligned all Budget Models with FNS Strategy Map and Project Portfolio
- Developed FNS Staffing Plan and Organizational Development Plan; and aligned them with the NICE Initiative
- Developed FISM approval and publication process. Released FISM 11-01 (TIC 2.0 Architecture) and FISM 11-02 (FISMA reporting instructions for 2011)

Homeland Security